Studi Tentang Kriptografi Simetris: Desain Algoritma *Block Cipher* dengan Skema Transposisi pada Kubus Rubik

Laporan Penelitian

Diajukan kepada
Fakultas Teknologi Informasi
untuk Memperoleh Gelar Sarjana Komputer

Peneliti:

Vania Beatrice Liwandouw
(672012224)

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga

Mei 2016

Studi Tentang Kriptografi Simetris: Desain Algoritma *Block Cipher* dengan Skema Transposisi Kubus Rubik

Laporan Penelitian

Diajukan kepada
Fakultas Teknologi Informasi
untuk Memperoleh Gelar Sarjana Komputer

Peneliti:

Vania Beatrice Liwandouw

(672012224)

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga
Mei 2016

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : VANIA BEATRICE LIWANDOUW

NIM : 672012224 Email : Vania.liwandouw@gmail.com

Fakultas : TEKNOLOGI INFORMASI Program Studi : TEKNIK INFORMATIKA

Judul tugas akhir : STUDI TENTANG KRIPTOGRAFI SIMETRIS : DESAIN ALGORITMA BLOCK CIPHER DENGAN SKEMA TRANSPOSISI KUBUS RUBIK

Pembimbing : 1. ALB DANNY WOWOR, S.Si., M.Cs

2. _____

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 17 JUNI 2016

Tanda tangan & nama terang mahasiswa

Vania Beatrice Uwandouw

F-LIB-080

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : VANIA BEATRICE LIWANDOUW

NIM : 672012224 Email : Vania.Liwandouw@gmail.com

Fakultas : TEKNOLOGI INFORMASI Program Studi : TEKNIK INFORMATIKA

Judul tugas akhir : STUDI TENTANG KRIPTOGRAFI SIMETRU : DESAIN ALGORITMA BLOCK CIPHER DENGAN SKEMA TRANSPOSISI PADA KUBUS RUBIK

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-ekslusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 17 JUNI 2016

VANIA BEATRICE LIWANDOUW
Tanda tangan & nama terang mahasiswa

Mengetahui,

ALB. DANNY WOWOR
Tanda tangan & nama terang pembimbing I

Tanda tangan & nama terang pembimbing II

F-LIB-081

Lembar Persetujuan

Studi tentang Kriptografi Simetris : Desain Algoritma Block Cipher dengan Skema Transposisi Kubus Rubik

Laporan Penelitian

Peneliti:

Vania Beatrice Liwandouw (672012224)

Telah disetujui untuk diuji:

Tanggal: 10 JUNI 2016

Alz Danny Wowor, S.Si., M.Cs.

Pembimbing

Lembar Pengesahan

Judul Tugas Akhir	: Studi Tentang Kriptografi Simetris: Desain Algoritma *Block Cipher* dengan Skema Transposisi pada Kubus Rubik
Nama Mahasiswa	: Vania Beatrice Liwandouw
NIM	: 672012224
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Informasi

Menyetujui,

Alz Danny Wowor, S.Si., M.Cs.
Pembimbing

Mengesahkan,

Dr. Dharmaputra T. Palekahelu, M.Pd.
Dekan

Suprihadi, S.Si., M.Kom.
Ketua Program Studi

Dinyatakan Lulus Ujian tanggal: 10 Juni 2016

Penguji:

1. Prof. Ir. Danny Manongga, M.Sc., Ph.D.
2. Prof. Dr. Ir. Eko Sediyono, M.Kom

Bukankah telah Kuperintahkan kepadamu: kuatkan dan teguhkanlah hatimu? Janganlah kecut dan tawar hati, sebab TUHAN, Allahmu, menyertai engkau, ke manapun engkau pergi

(Yosua 1 : 9)

Tulisan ini, ku persembahkan kepada Tuhan Yesus Kristus, papa, mama, vika, viki, oma, dan orang yang kucintai.

Kata Pengantar

Some people come in your life as blessings,
other come in your life as lessons. (Mother Theresa)

Penelitian teoritikal pada ranah fundamental merupakan studi yang dibutuhkan sebagai titik pijakan menuju pada kajian aplikatif. Pada ilmu komputer, algortima menjadi *domain* yang penting untuk menjadi relasi dan fungsi menuju pada aplikasi berupa *tools* (*software*) yang menjadi *kodomain* ataupun *range*.

Studi algoritma kriptografi sebagai pijakan untuk merancang sebuah *tools* pengamanan informasi juga perlu dilakukan. Kebutuhan algortima kriptografi mengalami transformasi sejak alat komunikasi yang digunakan manusia juga mengalami perubahan. Banyak studi yang lebih memperhatikan bagaimana merancang *tools* yang dapat diterapkan sebagai aplikasi *web* ataupun aplikasi *mobile* yang mendukung aktifitas manusia. Tetapi aplikatif akan menjadi sia-sia apabila kajian algoritma terhadap analisis kontekstual kekinian terutama kriptanalisis dan ruang kunci tidak diperhatikan.

Penelitian ini dilakukan memperhatikan aspek transposisi dan subtitusi guna melihat faktor ruang kunci, yang menjadi ukuran peradaban perkembangan kriptografi pada saat ini. Oleh karena itu, penelitian yang dilakukan terdiri dari dua algoritma kriptografi dan dirancang berbasis pada kunci simetris dengan skema *block* cipher.

Algoritma pertama menekankan pada skema transposisi, kemudian dikembangkan pada penelitian kedua yang memperhatikan proses transposisi dan juga subtitusi guna pemenuhan akan prinsip Shannon.

Kedua tulisan ini merupakan hasil kaloborasi dalam penelitian bersama Alz Danny Wowor yang dilakukan secara terpisah dan terpublikasi di seminar nasional pada tahun 2015. Penelitian pertama dengan judul "Desain Algoritma Berbasis Kubus Rubik dalam Perancangan Kriptografi Simetris" pada Seminar Teknik Informatika dan Sistem Informasi (SeTISI) di Universitas Kristen Maranatha, Bandung. Penelitian kedua yang berjudul "Kombinasi Algoritma Rubik, CSPRNG Chaos, dan S-Box Fungsi Linier dalam Perancangan Kriptografi Cipher Blok" dipublikasikan pada Seminar Nasional Sistem Informasi Indonesia (SESINDO) di Institut Teknologi Sepuluh Nopember Surabaya, dan berhasil terpilih sebagai *best paper* pada seminar nasional tersebut.

Laporan penelitian ini merangkum kedua penelitian yang diberikan pada bab yang berbeda. Sebagai pemenuhan akan *state of the art* maka sebagai pengantar yang diberikan pada bab pertama sebagai *general introduction* guna melihat masalah yang melatarbelakangi kedua penelitian ini. Setiap masalah dirangkum dalam sintesa-sintesa yang terjawab secara khusus diberikan pada bagian kedua dan bagian ketiga. Simpulan pada bagian terakhir dibuat menjadi sebuah *general discussion.* Bagian ini mencoba

membahas sintesa yang ada pada bagian awal sebagai simpulan dari kedua penelitan yang dilakukan.

Penelitian yang dilakukan dan tertuang dalam tulisan dengan format laporan penelitian ini, dapat dibuat dan terselesaikan hanya karena berkat dan tuntunan Tuhan Yesus Kristus. Tentunya juga atas dukungan serta doa dari orang-orang tercinta. Semoga tulisan ini dapat meberikan kontribusi dalam ranah algoritma kriptografi simetris. Sangat disadari bahwa tulisan ini merupakan embrio yang sedang berkembang menuju dan berjalan pada perbaikan yang masih jauh dari kesempurnaan, oleh karena itu berbagai kritik dan saran sangat diharapkan dan akan diterima dengan baik. Akhir kata, kiranya skripsi ini dapat bermanfaat dan berguna untuk kemajuan ilmu pengetahuan di masa yang akan datang. Tuhan Memberkati.

Salatiga, Juni 2016

Vania Beatrice Liwandouw

Abstrak

Kriptografi simetris khususnya block cipher sebagai sebuah algoritma pengamanan informasi memiliki keunggulan dari sisi efesiensi waktu dan dapat diimplementasikan di semua platform. Penelitian ini melakukan studi tentang block cipher khususnya proses transposisi menggunakan kubus rubik 4×4×4. *Selain transposisi, studi ini memperhatikan proses subtitusi dan ruang kunci sebagai ukuran kompleksitas waktu yang diperlukan.*

Metode transposisi yang dirancang pada kubus rubik 4×4×4 *sebagai media untuk menempatkan bit pada setiap sisi kubus rubik, sehingga total bit dalam sebuah kubus adalah* 384 *bit. Transposisi unik hasil dari perputaran yang dilakukan secara horizontal dan vertikal memberikan cipherteks yang secara grafik sangat fluktuatif. Kondisi ini menujukkan algoritma yang dirancang memberikan efek diffusion antara plainteks dan cipherteks.*

Studi selanjutnya menambah proses subtitusi untuk melengkapi pemenuhan prinsip confussion. Fokus hanya pada satu bagian yaitu keacakan tidaklah cukup dalam rancangan algoritma kriptografi, sebab transposisi hanya merubah posisi objek dan tidak merubah nilai. Kombinasi transposisi dan subtitusi mampu membuat algoritma dapat memenuhi prinsip Shannon, dan mengatasi uji ekstrim. Selain itu untuk memperbesar ruang kunci, dilakukan pembangkitan kunci dengan CSPNRG berbasis Chaos.

Studi kriptografi simetris terkait desain algoritma blok cipher dengan Skema Transposisi pada Kubus Rubik memenuhi prinsip Shannon, lolos uji kunci lemah, S-Box, dan Iterated Cipher. Selain itu, penggunaan ruang kunci 384 *bit akan menyulitkan kriptanalisis untuk melakukan uji brute force attack, sehingga akan dapat menahan serangan exhaustive key search dengan teknologi saat ini. Berdasarkan hal tersebut, rancangan ini dapat direkomendasikan sebagai kriptosistem dalam pengamanan informasi pada tataran studi sebuah algoritma.*

Keywords: *Kriptografi Simetris, Blok Cipher, Transposisi, Subtitusi, CSPNRG Chaos, Kubus Rubik* 4×4×4.

Daftar Isi

Halaman

Daftar Tabel

Halaman

Daftar Gambar

Halaman